在WAP121和WAP321接入点上配置802.1X身份验证

目标

在802.1X身份验证中，当主机（也称为请求方）尝试连接到安全网络时，称为身份验证方的网络设备会与支持安全协议RADIUS和可扩展身份验证协议(EAP)的身份验证服务器进行检查，以验证请求方的身份。这样，网络设备就为网络提供了额外的安全层。

本文档介绍如何将WAP121和WAP321接入点配置为802.1X身份验证的请求方。

适用设备

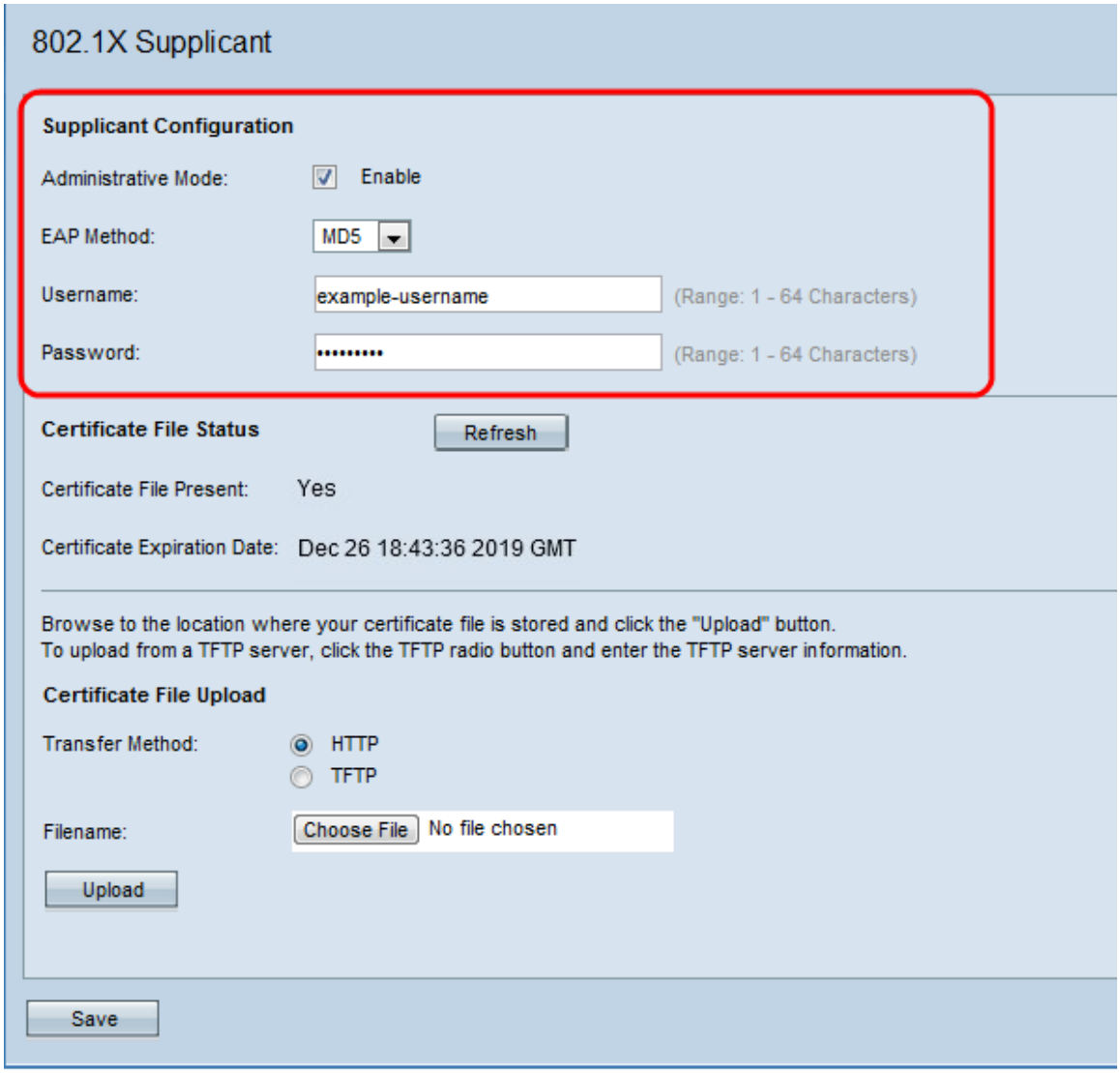
·WAP121
· WAP321

软件版本

•1.0.3.4

802.1X请求方配置

步骤1.登录Web配置实用程序，然后选择**System Security > 802.1X Supplicant客户端**。“请*求方配置*”页打开：



步骤2.在Administrative Mode字段中选中**Enable**，使设备能够在802.1X身份验证中充当请求方。

步骤3.从EAP Method字段的下拉列表中选择适当类型的可扩展身份验证协议(EAP)方法。

·MD5 - MD5是一种算法，用于加密任何大小到128位的数据，MD5算法使用公钥密码体制加密数据。

·PEAP — 受保护的EAP是一种身份验证方法，提供增强的安全性，PEAP通过服务器颁发的数字证书对无线局域网客户端进行身份验证，方法是在客户端和身份验证服务器之间创建加密的SSL/TLS隧道。

·TLS — 传输层安全(TLS)是一种加密协议，可为Internet通信提供安全性和数据完整性。当服务器和客户端通信时，TLS确保没有第三方篡改原始消息。MD5的大多数功能都用于TLS。

步骤4.在Username和Password字段中输入接入点用于从802.1X身份验证器获取身份验证的用户名和密码。用户名和密码的长度必须介于1到64个字母数字和符号字符之间。

第 5 步： 点击 **Save（保存），以保存设置。**

注意：Certificate File Status区域显示证书文件是否存在。SSL证书是证书颁发机构数字签名的证书，它允许Web浏览器与Web服务器进行安全通信。要管理和配置SSL证书，请参阅*WAP121和WAP321接入点上的安全套接字层(SSL)证书管理文章*。